Apparatus for the implementation of a system for the secure exchange of data according to the RSA method limited to digital signatures and message verification.

Patent number: EP0675614
Publication date: 1995-10-04
Inventor: FERREIRA RONALD (FR); HOPPE JOSEPH (FR)
Applicant: TRT TELECOM RADIO ELECTR (FR); PHILIPS ELECTRONICS NV (NL)
Classification:
- International: H04L9/32
- european: G07F7/10E; H04L9/32
Application number: EP19950200701 19950322
Priority number(s): FR19940003773 19940330

Also published as:
US5748782 (A1)
JP7287514 (A)
FR2718311 (A1)
EP0675614 (B1)

Cited documents:
XP000383974
XP000311977

Abstract of **EP0675614**

The device uses a physically secure microcomputer (1) which includes a microprocessor (2), a volatile memory (3) and a permanent memory (4) holding the operating instructions. An EEPROM memory (5) contains the secret code for the card, and the public code required for information exchange.
The device uses RSA encryption coding and requires authentication of a digital signature before encoding or decoding of the data. Each message must have a required structure before it can be transmitted, and application of the signature to the message only occurs if the message structure has been validated.